

**ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN  
BARNYARD2 PADA VPS UBUNTU**



Skripsi

Disusun sebagai salah satu syarat menyelesaikan jenjang Strata 1  
Pada Program Studi Informatika Fakultas Komunikasi dan Informatika  
Universitas Muhammadiyah Surakarta

**Oleh :**

Alim Nuryanto

L200110022

**PROGRAM STUDI INFORMATIKA  
FAKULTAS KOMUNIKASI DAN INFORMATIKA  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

**2015**

**ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN  
BARNYARD2 PADA VPS UBUNTU**



Skripsi

Disusun sebagai salah satu syarat menyelesaikan jenjang Strata 1  
Pada Program Studi Informatika Fakultas Komunikasi dan Informatika  
Universitas Muhammadiyah Surakarta

**Oleh :**

Alim Nuryanto

L200110022

**PROGRAM STUDI INFORMATIKA  
FAKULTAS KOMUNIKASI DAN INFORMATIKA  
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

**2015**

**HALAMAN PERSETUJUAN USULAN PENELITIAN**

Skripsi dengan judul

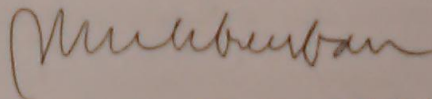
**ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, BARNYARD2  
PADA VPS UBUNTU**

Telah disetujui pada :

Hari : Jum'at

Tanggal : 24 Juli 2015

Pembimbing 1



(Muhammad Kusban, S.T, M.T)

NIK : 663

SKRIPSI

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, BARNYARD2

PADA VPS UBUNTU

Dipersiapkan dan disusun oleh :

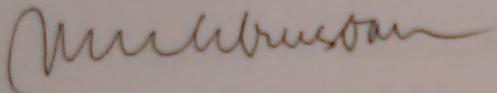
Alim Nuryanto

L200110022

Pada tanggal 30 Juli 2015

Susunan Dewan Penguji

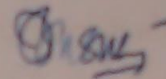
Pembimbing I



Muhammad Kusban, S.T, M.T

NIK. 663

Dewan Penguji I



Agus Ulinuha, S.T, M.T, Ph.D

NIK : 656

Dewan Penguji II



Dr. Heru Supriyono, M.Sc

NIK : 970

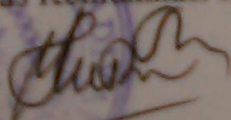
Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 7 Agustus 2015

Dekan

Fakultas Komunikasi Informatika

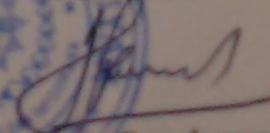


Husni Thamrin, S.T., M.T., Ph.D.

NIK. 706

Ketua Program Studi

Informatika



Dr. Heru Supriyono, M.Sc.

NIK. 970



## KONTRIBUSI

Dengan ini, peneliti menyatakan dengan sebenarnya bahwa Karya ini murni hasil dari penelitian sendiri dan sepengetahuan peneliti tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam menyusun skripsi :

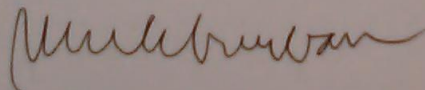
1. Peneliti melakukan penelitian aplikasi ini sendiri dengan bantuan buku, dan internet.
2. Software yang peneliti gunakan dalam pembuatan aplikasi adalah Suricata, Snorby, dan Barnyard2 dengan perangkat komputer pribadi.
3. Sistem operasi yang digunakan dalam penelitian adalah windows 7 64-bit dan Ubuntu LTS 12.04.

Apabila ternyata kelak ditemukan hari terbuktinya ada ketidakbenaran dalam pernyataan maka peneliti akan sepenuhnya bertanggungjawab sepenuhnya.

Surakarta, 2 Agustus 2015

Mengetahui

Pembimbing Tugas Akhir ,



**Muhammad Kusban, S.T, M.T**

**NIK : 663**

Penulis



**Alim Nuryanto**

**NIM : L200110022**

## HALAMAN PERSEMBAHAN

Puji syukur peneliti panjatkan kehadiran Allah SWT, yang telah memberikan kesempatan kepada peneliti untuk menyelesaikan skripsi dengan judul “Analisis dan Implementasi Suricata, Snorby, dan Barnyard2 pada VPS Ubuntu“. Shalawat serta salam peneliti panjatkan kepada Nabi besar Muhammad SAW karena beliau adalah yang telah memimpin Umat Islam dari jaman kebodohan ke jaman penuh pengetahuan. Peneliti mempersembahkan karya ini kepada :

1. Kedua orang peneliti Sumaryono dan Setiani yang telah memberikan dukungan penuh kepada peneliti untuk menyelesaikan skripsi ini,
2. Muhammad Kusban, S.T, M.T yang telah membimbing peneliti dalam pengerjaan skripsi ini,
3. Teman - teman seangkatan ataupun beda angkatan yang menimba ilmu di Universita Muhammadiyah Surakarta yang tidak dapat peneliti sebutkan namanya satu - persatu.

Peneliti menyadari bahwa banyak kekurangan dari penyusunan skripsi ini. Namun, peneliti berharap skripsi ini dapat membantu menjadi referensi ataupun sebagai salah informasi yang dapat dimanfaatkan dengan baik oleh para pembaca.

## KATA PENGANTAR

Puji syukur peneliti panjatkan kehadiran Allah SWT, yang telah menciptakan langit dan Bumi beserta isinya serta melimpahkan berbagai macam ilmu pengetahuan yang tidak terhitung jumlahnya. Shalawat serta salam peneliti panjatkan kepada Nabi besar Muhammad SAW karena beliau adalah yang telah memimpin Umat Islam dari jaman kebodohan ke jaman penuh pengetahuan.

Skripsi dengan judul “Analisis dan Implementasi Suricata, Snorby, dan Barnyard2 pada VPS Ubuntu” disusun sebagai salah satu persyaratan akhir untuk mendapatkan gelar Sarjana di Universitas Muhammadiyah Surakarta pada Fakultas Komunikasi dan Informatika. peneliti mengucapkan terimakasih kepada :

1. Bapak Husni Tamrin, S.T, M.T selaku Dekan Fakultas Informatika Universitas Muhammadiyah Surakarta yang telah menandatangani halaman pengesahan makalah skripsi ini,
2. Bapak Dr. Heru Supriyono, S.T, M.T selaku Ketua Prodi Jurusan Informatika Universitas Muhammadiyah Surakarta yang telah menandatangani halaman pengesahan makalah skripsi ini,
3. Ibu Umi Fadlilah, S.T, M.Eng selaku Sekretari Praktek Prodi Jurusan Informatika Universitas Muhammadiyah Surakarta yang telah membantu peneliti dalam menyelesaikan laporan Kerja Praktek sebelumnya,
4. Bapak Fatah Yasin Irsyadi, S.T, M.T selaku Koordinator Kerja Praktek Prodi Jurusan Informatika Universitas Muhammadiyah Surakarta yang telah menjadi dosen pengajar,
5. Bapak Muhammad Kusban, S.T, M.T selaku dosen dan pembimbing skripsi peneliti yang telah membimbing peneliti sehingga skripsi dapat

terselesaikan,

6. Dosen - dosen FKI Prodi Informatika yang telah mengajar dan memberikan pengetahuan kepada peneliti selama menempuh proses perkuliahan,
7. Adjie Sapetra, S.Kom selaku Koordinator Skripsi Prodi Informatika Fakultas Teknik Informatika yang selalu memberikan informasi berkaitan dengan proses pembuatan skripsi,
8. Kedua orang tua yang selalu mendukung peneliti untuk menyelesaikan skripsi ini dengan baik,
9. Teman - teman FKI angkatan 2011.

Sekali lagi peneliti mengucapkan terimakasih kepada beliau - beliau beserta teman - teman yang tentunya tidak dapat peneliti sebutkan satu persatu.

Surakarta, 24 Juli 2015

Alim Nuryanto

L200110022



## ABSTRAK

*Server* merupakan perangkat yang telah ter-integrasi dengan spesifikasi *hardware* tertentu, dan *software* yang memiliki fungsi tertentu seperti ftp, ssh, web server. Layanan tersebut rentan akan serangan yang dapat menimbulkan kerugian. Oleh karena itu diperlukan sistem pendukung yang mampu mendeteksi sebuah aktifitas jaringan. Suricata adalah IDS yang mampu mendeteksi sebuah aktifitas jaringan dan mengidentifikasi ancaman serangan dibantu dengan *rules* yang ter-integrasi. Suricata memindai setiap datagram yang dikirim pada sesi TCP dan mengubah menjadi informasi dan dikirim pada aplikasi Snorby untuk diolah. *Rules* pada suricata berperan dalam mengidentifikasi serangan yang terjadi pada sebuah host.

Kata kunci : Server, *Suricata*, *Snorby*, *Rules*, *IDS*,

## DAFTAR ISI

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU.....	ii
HALAMAN PERSETUJUAN USULAN PENELITIAN.....	iii
HALAMAN PENGESAHAN.....	iv
KONTRIBUSI.....	v
HALAMAN PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
ABSTRAK.....	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xv
DAFTAR SINGKATAN.....	xix
BAB 1.....	1
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah.....	2
1.4. Tujuan Penelitian.....	3
1.5. Manfaat Penelitian.....	3
1.6. Sistematika penelitian laporan.....	3
BAB 2.....	5
2.1. Landasan Teori.....	5
BAB 3.....	9
3.1 Metode Penelitian.....	9

3.2. Waktu dan Tempat.....	9
3.3. Peralatan Utama dan Pendukung.....	9
3.4. Alur Penelitian.....	10
3.4.1. Instalasi Snorby.....	12
3.4.2. Instalasi Suricata.....	17
3.4.3. Instalasi Barnyard2.....	21
3.4.4. Pengujian Request Packet Data ke <i>Server 1</i> .....	23
3.4.5 Pengujian <i>scanning</i> menggunakan Nmap pada <i>Server 1</i> .....	23
3.4.6 Pengujian Menggunakan Tool Hydra.....	25
3.4.7 Pengujian menggunakan sqlmap.....	27
3.4.8 Pengujian menggunakan metasploit konsol.....	28
BAB 4.....	30
4.1 Hasil Penelitian.....	30
4.1.1 Hasil Pengujian <i>Request Packet Data</i> ke <i>Server 1</i> .....	30
4.1.2 Hasil Pengujian Scanning Menggunakan Nmap Pada <i>Server 1</i> .....	44
4.1.3 Hasil Pengujian Menggunakan Tool Hydra.....	56
4.1.4 Pengujian Menggunakan Tool Sqlmap.....	66
4.1.5 Pengujian Menggunakan Metasploit Konsol.....	69
4.2 Pembahasan.....	71
4.2.1 Analisis Kebutuhan Sistem.....	71
4.2.2 Analisis Pengujian Request Packet Data Pada <i>Server 1</i> .....	73
4.2.3 Analisis Pengujian Scanning Menggunakan Nmap Pada <i>Server 1</i> ...	73
4.2.4 Analisis Pengujian Tool Hydra.....	74
4.2.5 Analisis Pengujian Menggunakan Tool Sqlmap.....	75
4.2.6 Analisis Pengujian Menggunakan Metasploit Konsol.....	76

BAB 5.....	77
5.1 Kesimpulan.....	77
5.2 Saran.....	77
DAFTAR PUSTAKA.....	78

## DAFTAR TABEL

Tabel 3.1 <i>Request Packet Data</i> .....	23
Tabel 3.2 <i>Reply Packet Data</i> .....	23
Tabel 3.3 Daftar Perintah Nmap.....	24
Tabel 3.3 (Lanjutan).....	25
Tabel 3.4 Waktu pengujian.....	25
Tabel 3.4 (Lanjutan).....	26
Tabel 3.5 <i>World List User</i> .....	26
Tabel 3.6 <i>World List Password</i> .....	26
Tabel 3.7 Daftar Pengujian Menggunakan Metasploit Konsol.....	28
Tabel 4.1 <i>Capture 1 IP Header</i> Tanggal 12 Juli 2015 Pengujian Jam 5:10- 5:20 .....	30
Tabel 4.1 (Lanjutan).....	31
Tabel 4.2 Hasil <i>Capture 1 ICMP Header</i> Tanggal 12 Juli 2015 Jam 5:10- 5:20	31
Tabel 4.2 (Lanjutan).....	32
Tabel 4.3 Hasil <i>Capture 2 IP Header</i> Tanggal 12 Juli 2015 Pengujian Jam 6:01- 6:11.....	32
Tabel 4.4 Hasil <i>Capture 2 ICMP Header</i> Tanggal 12 Juli 2015 Pengujian Jam 6:01- 6:11.....	33
Tabel 4.5 <i>Capture 3 IP Header</i> Tanggal 12 Juli 2015 Pengujian Jam 18:59 - 19:09.....	33
Tabel 4.5 (Lanjutan).....	34
Tabel 4.6 <i>Capture 3 ICMP Header</i> Tanggal 12 Juli 2015 Pengujian Jam 18:59 - 19:09.....	34

Tabel 4.7 <i>Capture 4 IP Header</i> Tanggal 13 Juli 2015	
Pengujian Jam 3:46 - 3:56.....	35
Tabel 4.8 <i>Capture 4 ICMP Header</i> Tanggal 13 Juli 2015	
Pengujian Jam 3:46 - 3:56.....	36
Tabel 4.9 <i>Capture 1 IP Header</i> Tanggal 15 Juli 2015 Jam 10:00.....	45
Tabel 4.10 <i>Capture 1 TCP Header</i> Tanggal 15 Juli 2015 Jam 10:00.....	45
Tabel 4.10 (Lanjutan).....	46
Tabel 4.11 <i>Capture 2 IP Header</i> Tanggal 15 Juli 2015 Jam 10:20.....	46
Tabel 4.12 <i>Capture 2 TCP Header</i> Tanggal 15 Juli 2015 Jam 10:20.....	46
Tabel 4.12 (Lanjutan).....	47
Tabel 4.13 <i>Capture 3 IP Header</i> Tanggal 15 Juli 2015 Jam 11:00.....	47
Tabel 4.14 <i>Capture 3 UDP Header</i> Tanggal 15 Juli 2015 Jam 11:00.....	47
Tabel 4.14 (Lanjutan).....	48
Tabel 4.15 <i>Capture 3 TCP Header</i> Tanggal 15 Juli 2015 Jam 11:00.....	48
Tabel 4.16 <i>Capture 4 IP Header</i> Tanggal 15 Juli 2015 Jam 18:10.....	48
Tabel 4.17 <i>Capture 4 TCP Header</i> Tanggal 15 Juli 2015 Jam 18:10.....	49
Tabel 4.18 Pengujian Layanan <i>Server 1 IP Header Capture</i> .....	57
Tabel 4.18 (Lanjutan).....	58
Tabel 4.19 Pengujian Layanan <i>Server 1 TCP Header</i> .....	58
Tabel 4.19 (Lanjutan).....	59
Tabel 4.20 <i>IP Header</i> Pengujian <i>Sqlmap</i> .....	66
Tabel 4.20 (Lanjutan).....	67
Tabel 4.21 <i>TCP Header</i> Pengujian <i>Sqlmap</i> .....	67
Tabel 4.20 Pengujian Menggunakan Metasploit <i>IP Header</i> .....	69
Tabel 4.21 Pengujian Menggunakan Metasploit <i>TCP Header</i> .....	69



## DAFTAR GAMBAR

Gambar 3.1 Diagram Alir.....	11
Gambar 3.2 Topologi Jaringan.....	12
Gambar 3.3 Konfigurasi file database.yml.....	14
Gambar 3.3 Konfigurasi file snorby_config.yml.....	14
Gambar 3.4. Konfigurasi file my.cnf.....	15
Gambar 3.6. File snorby.....	16
Gambar 3.7 Form Login Snorby.....	17
Gambar 3.8 Install libraries <i>Server 1</i> .....	18
Gambar 3.9 Instalasi HTP libraries.....	18
Gambar 3.10 log suricata.....	21
Gambar 3.11 Arsitektur cara kerja nmap.....	24
Gambar 3.12 <i>Scanning</i> menggunakan Nmap.....	25
Gambar 3.13 <i>Brute Force Attack</i> menggunakan Hydra.....	27
Gambar 3.14 serangan menggunakan sqlmap.....	27
Gambar 3.15 Serangan pada vsftpd <i>Server 1</i> .....	29
Gambar 4.1 Diagram Versi <i>IP Header</i> .....	37
Gambar 4.2 Diagram <i>Header Length IP Header</i> .....	37
Gambar 4.3 Diagram <i>Type Of Service IP Header</i> .....	38
Gambar 4.4 Diagram <i>Total Length IP Header</i> .....	38
Gambar 4,5 Diagram <i>Identifier IP Header</i> .....	39
Gambar 4.6 Diagram <i>Flag IP Header</i> .....	39
Gambar 4.7 Diagram <i>Fragment Offset IP Header</i> .....	40
Gambar 4.8 Diagram <i>Time To Live IP Header</i> .....	40

Gambar 4.9 Diagram Protokol <i>IP Header</i> .....	41
Gambar 4.10 Diagram <i>Header Checksum IP Header</i> .....	41
Gambar 4.11 Diagram <i>Type ICMP Header</i> .....	42
Gambar 4.12 Diagram <i>Code ICMP Header</i> .....	42
Gambar 4.13 Diagram <i>Checksum ICMP Header</i> .....	43
Gambar 4.14 Diagram <i>Identifier ICMP Header</i> .....	43
Gambar 4.15 Diagram <i>Sequence Number ICMP Header</i> .....	44
Gambar 4.16 Pengujian Nmap Versi <i>IP Header</i> .....	50
Gambar 4.17 Pengujian Nmap <i>H.Length IP Header</i> .....	50
Gambar 4.18 Pengujian Nmap <i>TOS IP Header</i> .....	50
Gambar 4.19 Pengujian Nmap <i>Length IP Header</i> .....	51
Gambar 4.20 Pengujian Nmap <i>Identifier IP Header</i> .....	51
Gambar 4.21 Pengujian Nmap <i>Identifier IP Header</i> .....	51
Gambar 4.22 Pengujian Nmap <i>Offset IP Header</i> .....	52
Gambar 4.23 Pengujian Nmap <i>TTL IP Header</i> .....	52
Gambar 4.24 Pengujian Nmap Protokol <i>IP Header</i> .....	52
Gambar 4.25 Pengujian Nmap Protokol <i>IP Header</i> .....	53
Gambar 4.26 Pengujian Nmap Src.Port <i>TCP Header</i> .....	53
Gambar 4.27 Pengujian Nmap Dst.Port <i>TCP Header</i> .....	53
Gambar 4.28 Pengujian Nmap Seq <i>TCP Header</i> .....	54
Gambar 4.29 Pengujian Nmap Ack <i>TCP Header</i> .....	54
Gambar 4.30 Pengujian Nmap Offset <i>IP Header</i> .....	54
Gambar 4.31 Pengujian Nmap Res <i>TCP Header</i> .....	55
Gambar 4.32 Pengujian Nmap Flags <i>TCP Header</i> .....	55
Gambar 4.33 Pengujian Nmap Flags <i>TCP Header</i> .....	55

Gambar 4.34 Pengujian Nmap Flags <i>TCP Header</i> .....	56
Gambar 4.35 Pengujian Nmap URP <i>TCP Header</i> .....	56
Gambar 4.36 Pengujian Hydra Versi <i>IP Header</i> .....	60
Gambar 4.37 Pengujian Hydra <i>H.Length IP Header</i> .....	60
Gambar 4.38 Pengujian Hydra TOS <i>IP Header</i> .....	60
Gambar 4.38 Pengujian Hydra <i>Length IP Header</i> .....	61
Gambar 4.39 Pengujian Hydra <i>ID IP Header</i> .....	61
Gambar 4.40 Pengujian Hydra <i>Flags IP Header</i> .....	61
Gambar 4.41 Pengujian Hydra <i>Offset IP Header</i> .....	62
Gambar 4.42 Pengujian Hydra TTL <i>IP Header</i> .....	62
Gambar 4.43 Pengujian Hydra Protokol <i>IP Header</i> .....	62
Gambar 4.44 Pengujian Hydra Csum <i>IP Header</i> .....	63
Gambar 4.45 Pengujian Hydra <i>Src,Port TCP Header</i> .....	63
Gambar 4.46 Pengujian Hydra <i>Dst.Port TCP Header</i> .....	63
Gambar 4.47 Pengujian Hydra <i>Seq TCP Header</i> .....	64
Gambar 4.48 Pengujian Hydra <i>Ack TCP Header</i> .....	64
Gambar 4.49 Pengujian Hydra <i>Offset TCP Header</i> .....	64
Gambar 4.50 Pengujian Hydra <i>Res TCP Header</i> .....	65
Gambar 4.51 Pengujian Hydra <i>Flags TCP Header</i> .....	65
Gambar 4.52 Pengujian Hydra <i>Window TCP Header</i> .....	65
Gambar 4.53 Pengujian Hydra <i>Csum TCP Header</i> .....	66
Gambar 4.54 Pengujian Hydra <i>URP TCP Header</i> .....	66
Gambar 4.55 Ver, Hlen, Tos, ID, Flags, Off, TTL, Proto IP Header Pengujian Sqlmap.....	67
Gambar 4.56 <i>Len, Csum IP Header</i> .....	68

Gambar 4.56 Src.Port, Dst.Port, <i>Csum TCP Header</i> .....	68
Gambar 4.57 Seq, Ack, Off, Res, Flags, Win, URP <i>TCP Header</i> .....	68
Gambar 4.58 Ver, Hlen, Tos, Flags, Offset, TTL <i>IP Header</i> .....	70
Gambar 4.58 Length, ID, <i>Csum IP Header</i> .....	70
Gambar 4.59 Src.Port, Window, <i>Csum TCP Header</i> .....	70
Gambar 4.60 Dst.Port, Offset, Res, Flags, URP <i>TCP Header</i> .....	71
Gambar 4.61 Seq, Ack <i>TCP Header</i> .....	71

## DAFTAR SINGKATAN

ACK	: <i>Acknowledgment</i>
Csum	: Cheksum
Dst. Port	: <i>Destination Port</i>
HLEN	: <i>Header Length</i>
ID	: <i>Identifier</i>
IDS	: <i>Information Detection System</i>
Len	: <i>Total Length</i>
Off	: Data Offset
Offset	: Fragment Offset
Proto	: Protokol
Seq	: Sequence
Src. Port	: <i>Source Port</i>
TOS	: <i>Type Of Service</i>
TTL	: <i>Time To Live</i>
URP	: <i>Urgent Pointer</i>
Ver	: Versi
Win	: <i>Window</i>